Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act

Ann Cavoukian, Ph.D.
Commissioner
October 2005

Information and Privacy Commissioner/Ontario

Privacy Impact Assessment Guidelines
for the *Ontario Personal Health Information Protection Act*

Ann Cavoukian, Ph.D.
Commissioner
October 2005

Information and Privacy
Commissioner/Ontario

TABLE OF CONTENTS

1. Introduction and Overview 4

1.1 About the Information & Privacy Commissioner/Ontario (IPC) 4

1.2 Purpose of the *Privacy Impact Assessment (PIA) Guidelines* 4

1.3 What is a PIA? 4

1.4 Benefits of a PIA 5

1.5 Methodology for conducting a PIA 6

1.6 Criteria for a high-quality PIA 7

2. Getting Started 8

2.1 Are you a health information custodian? 8

2.2 Does your information system, technology or program involve personal health information? 8

2.3 Are you a health information network provider under *PHIPA*? 9

3. Questionnaire Instructions 10

3.1 Understanding how the questionnaire is organized 10

3.2 "Note fields" versus "enclosure references" 10

3.3 Organizational privacy management versus project privacy management 10

3.4 Components of the questionnaire 11

4. Privacy Impact Assessment Questionnaire – Annotated 12

Appendix A – PIA Questionnaire Template 25

Appendix B – Sample Methodologies for Conducting a PIA 35

Appendix C – Definition of "Personal Health Information" under *PHIPA* 36

Appendix D – Organization for Economic Co-operation and Development – Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 37

1 INTRODUCTION AND OVERVIEW

1.1 About the Information & Privacy Commissioner/Ontario (IPC)

The Ontario government has enacted the *Personal Health Information Protection Act, 2004* (*PHIPA*) – a provincial law that will help keep the personal health information of Ontarians in the custody or control of organizations in the health sector private, confidential and secure by imposing rules relating to its collection, use and disclosure and by requiring reasonable measures be undertaken to ensure it is protected against theft, loss and unauthorized use or disclosure. This privacy law came into effect on November 1, 2004. *PHIPA* designates the Information and Privacy Commissioner/Ontario (IPC) as being responsible for overseeing compliance with *PHIPA*'s provisions.

1.2 Purpose of the *Privacy Impact Assessment (PIA) Guidelines*

The IPC has developed these *Privacy Impact Assessment (PIA) Guidelines* as a self assessment tool to assist health information custodians in reviewing the impact that a proposed information system, technology or program[1] may have on the privacy of an individual's personal health information under *PHIPA*. The IPC recommends that health information custodians with significant existing information systems, technologies or programs involving personal health information, or adopting new systems, technologies or programs, strongly consider conducting a PIA to identify and mitigate privacy risks. This is because a PIA is a valuable due diligence exercise, in which a health information custodian identifies and addresses potential privacy risks that may occur in the course of operating a proposed or existing information system, technology or program. In addition, privacy impact assessments have become a standard part of the "best privacy practices" undertaken by many organizations in the health sector in other jurisdictions, as well as several health information custodians in Ontario.

The IPC understands that privacy impact assessments are *not* required under *PHIPA* for health information custodians. As such, health information custodians that use these guidelines to conduct a PIA will *not* be expected to submit their PIA to the IPC for review under *PHIPA*. However, the IPC may use any PIA as a starting point for any investigation into a breach of privacy under *PHIPA*.

1.3 What is a PIA?

A PIA is a formal risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology or program may have on individuals' privacy. A PIA also identifies ways in which privacy risks can be mitigated. A PIA is desirable to assess the following types of risks:

- Risks arising from a new technology or the convergence of existing technologies such as an electronic medical record (EMR) system or electronic health record (EHR) system;
- Risks arising from the use of a known privacy-intrusive technology in new circumstances, such as the installation of CCTV in patient examination rooms for teaching or educational purposes or the recording of telephone consultations with patients;
- Risks arising from a new program or from changing information handling practices with significant privacy effects, such as a proposal to use personal health information collected for treatment purposes to develop a research database or a proposal to integrate an EMR or EHR with a patient scheduling system; and
- Risks arising from legacy systems[2] that may not support privacy and security best practices. Best practices include, but are not limited to, auditing access to personal health information, providing access to personal health information based on a user's job requirements, and requiring individuals to sign into a system with a

1 The terms "information system," "technology," and "program" are intended to subsume the words "application," "project," "scheme," "initiative," as well as any other word or term that refers to a defined course of endeavour.

2 A "legacy system" is an existing information system or application in which an organization has already made a serious investment of time and resources. Many of Ontario's health information custodians store individuals' personal health information in information systems or applications that would be considered legacy systems. It is common for new information systems, technologies or programs to interface with legacy systems or to import historic personal health information from them.

unique username and password before they can access any personal health information.

References to the potential of privacy impact assessments can be found at least as early as 1989[3] and official guidelines for the preparation of privacy impact assessments date from 1991.[4] However, the practice of privacy impact assessments has significantly gathered pace since 1999 as its merits have been identified and the preparation of such assessments has become mandatory in certain circumstances. For example, the Alberta *Health Information Act* requires that the Information and Privacy Commissioner of Alberta receive a PIA for review and comment before an organization implements proposed administrative practices and information systems relating to the collection, use or disclosure of individually identifying health information.

1.4 Benefits of a PIA

A PIA has several benefits, including:

1) A PIA outlines data protection risks, which health information custodians are required to mitigate under *PHIPA*. (Note that while health information custodians may not be formally required to conduct a PIA under *PHIPA*, they are required to take steps that are reasonable to ensure that personal health information in their custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal);
2) A PIA functions as a tool to promote the systematic analysis of privacy issues in order to inform debate on proposed or existing information systems, technologies or programs;
3) A PIA helps the relevant decision-makers understand the risks associated with a proposed or existing information system, technology or program, thereby avoiding any adverse public reaction;
4) A PIA functions as a kind of "early warning device" to protect the reputation of the health information custodian considering implementing a new information system, technology or program;
5) A PIA brings responsibility clearly back to the proponents of the proposed or existing information system, technology or program and implies that such proponents must "own" and mitigate any adverse privacy effects;
6) A PIA serves to reduce costs when completed at the development stage since changes to meet privacy concerns, for instance by adopting privacy enhancing technologies, are cheaper at the design and early implementation phases, well before a system, technology or program is fully operational;
7) A PIA provides a credible source of information for health information custodians, privacy regulators, and the public – a PIA should not merely identify potential privacy problems with a proposed or existing information system, technology or program, it should also allay privacy concerns that might develop if no credible or detailed analysis were to be available; and
8) Finally, a PIA provides a cost-effective means for privacy regulators (e.g. the Information and Privacy Commissioners) to understand the data protection implications of a proposed or existing information system, technology or program without having to undertake expensive field research themselves.

3 See David Flaherty, *Protecting Privacy in Surveillance Societies*, 1989, page 405.

4 See State of New York Public Service Commission, "Statement of Policy on Privacy in Telecommunications," 22 March 1991, reprinted in the Information and Privacy Commissioner of Ontario's submission to the Ontario Telephone Service Commission "Privacy and Telecommunications," September 1992.

1.5 Methodology for Conducting a PIA

Methodologies for conducting privacy impact assessments vary, with certain organizations being required to follow specific methodologies, often as a result of particular privacy laws or policy requirements. For example, both the Alberta Information and Privacy Commissioner and the Ontario Management Board Secretariat have published specific instructions or guidelines to assist organizations in conducting a PIA. For a list of various PIA methodologies, see Appendix B - Sample Methodologies for Conducting a PIA.

These *PIA Guidelines* produced by the IPC provide an annotated questionnaire for health information custodians that are subject to *PHIPA*. The questionnaire requests information of two general types: that related to the health information custodian's organizational privacy management practices (10 questions) and that related specifically to the information system, technology or program (20 questions). Organizational privacy policy and procedures, or the lack of them, can be significant factors in the ability of a health information custodian to ensure that privacy protecting measures are available for specific information systems, technologies or programs. For this reason, these guidelines focus not only on specific information systems, technologies or programs that the health information custodian will describe in its responses to the questionnaire, but they also ask the health information custodian to examine organizational information practices[5] that could have an impact on the privacy of an individual's personal health information.

The questions in the guidelines are based on "best PIA practices" developed by established PIA experts such as David Flaherty, the former Information and Privacy Commissioner of British Columbia, and Blair Stewart, the Assistant Privacy Commissioner of New Zealand. In addition, the questions are similar in format and general content[6] to the PIA questionnaire produced by the Alberta Information and Privacy Commissioner on the assumption that, to the greatest extent possible, organizations in the health sector want to use tools that are consistent across jurisdictions, particularly as personal health information is likely to flow across provincial borders with increasing frequency in a rapidly evolving e-health environment[7].

These *PIA Guidelines* require a health information custodian to provide detailed information on the following topics:

- Organizational privacy management, including privacy policies, privacy controls and the privacy structure and organization at the health information custodian that is the major proponent of the proposed or existing information system, technology or program;
- Project privacy management, including a detailed description of:
    - the personal health information with which the proposed or existing information system, technology or program deals;
    - the sources from which this personal health infomation is to be obtained;
    - the circumstances in which personal health information collection is to take place;
    - the processing of personal health information;
    - the intended uses of the personal health information held or thus produced;
    - the proposed recipients and their intended use of the personal health information;
    - the circumstances in which personal health information processing, use and disclosure are to take place;
    - the safeguards which will be implemented to protect against unauthorized access, use, disclosure, modification or loss; and
    - any arrangements for audit and enforcement.

5 Section 2 of *PHIPA* defines "information practices," in relation to a health information custodian, to mean, the policy of the custodian for actions in relation to personal health information, including, (a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and (b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information.

106-01519/

1.6 Criteria for a High-Quality PIA[6]

A high-quality PIA must contain a detailed description of the personal health information collected, used, disclosed and retained for the proposed or existing information system, technology or program. In effect, the PIA "tells the story" of the information system, technology or program – why it is being or has been implemented and how it collects, uses, discloses and retains personal health information. In this process, the PIA uncovers and attempts to resolve specific privacy issues in a comprehensive manner on the basis of clear thinking and accurate information.

In "telling the story" of the proposed or existing information system, technology or program, a high-quality PIA should offer a consciously critical perspective as a means of raising awareness about the privacy risks associated with a proposed or existing information system, technology or program. There is sometimes a tendency for privacy impact assessments to "gloss over" privacy risks or to downplay their importance for fear of jeopardizing "progress," particularly when a PIA is conducted by internal resources who may have an important stake in the health information custodian's "successful" development or operations of the information system, technology or program. However, it is the function of a high-quality PIA to offer an informed, critical perspective in order to foster awareness about how a proposed or existing information system, technology or program actually works, the privacy risks it entails and how such risks may be mitigated. Such awareness often serves to anticipate and avert privacy crises as well as assist privacy oversight bodies (e.g. the board, senior management, auditors and/or the Commissioner) to better understand the merits and risks of particular information systems, technologies or programs.

A high-quality PIA should also accurately represent the legal standards for personal health information protection that must be met for health information custodians subject to *PHIPA* (or to other legislation if the information system, technology or program discloses personal health information outside of Ontario). However, the IPC also notes that health information custodians may choose to conduct a PIA for more than just "legal compliance" reasons. For example, the privacy expectations of patients or clients may warrant the conducting of a PIA even when a health information custodian is confident that its information system, technology or program complies with *PHIPA*.

For the reasons discussed above, these *PIA Guidelines* allow for responses in two forms. Checkboxes provide summary responses to the questions posed in the questionnaire. "Note fields" or free text fields provide for the elaboration of those responses as the author of the PIA feels is appropriate. In addition, the questionnaire has a column to provide for cross-references to separate enclosures on specific responses, which the author of the PIA may wish to include as supporting information. The completion of an effective and meaningful PIA requires a dialogue between the author of the PIA and the proponents, designers, builders and users of the proposed or existing information system, technology or program, which these guidelines are intended to facilitate.

6 The PIA Guidelines from the Ontario Information and Privacy Commissioner are customized for *PHIPA*. By contrast, the PIA Guidelines from the Alberta Information and Privacy Commissioner are intended for all public bodies subject to the *Health Information Act* and/or municipal and provincial public sector privacy legislation.

7 The IPC would like to thank and acknowledge the Alberta Information and Privacy Commissioner, Frank Work, for allowing the IPC to modify the Privacy Impact Assessment Questionnaire produced by the Office of the Information and Privacy Commissioner of Alberta in accordance with Ontario's *Personal Health Information Protection Act, 2004*.

8 The IPC gratefully acknowledges the work of David Flaherty in this section for his unpublished paper on PIA criteria for Canada Health Infoway Inc. (March 2005).

2 GETTING STARTED

2. Getting Started

It is considered a "best privacy practice" for organizations with significant existing information systems, technologies or programs that involve personal information, or adopting new systems, technologies or programs, to conduct a PIA. These *PIA Guidelines* are written specifically for health information custodians that are subject to *PHIPA* and have proposed or existing information systems, technologies or programs that involve personal health information. In order to maximize the value of these guidelines, you will first want to determine if *PHIPA* applies to your organization (see question 2.1 below) and, second, whether or not the proposed or existing information system, technology or program involves personal health information (see question 2.2). Lastly, you will want to determine whether or not your organization is one of those legally required under *PHIPA* to complete a privacy impact assessment (see question 2.3 below).

2.1 Are you a health information custodian?

PHIPA applies to health information custodians that collect personal health information on or after November 1, 2004 and to health information custodians that use or disclose personal health information after November 1, 2004. *PHIPA* also applies to persons and organizations that are not health information custodians but who have received personal health information from a health information custodian.

Question 2.1: Are you a health information custodian? *PHIPA* defines a "health information custodian" as a person or organization set out in section 3(1) of *PHIPA* who has custody or control of personal health information.

Examples of health information custodians in section 3(1) include a health care practitioner or a person who operates a group practice of health care practitioners that provide health care, hospitals, psychiatric facilities, long term care facilities, community care access corporations, pharmacies, laboratories, ambulance services and boards of health.

2.2 Does your information system, technology or program involve personal health information?

These *PIA Guidelines* are intended to help health information custodians identify and manage privacy risks associated with proposed or existing information systems, technologies or programs involving personal health information as defined under *PHIPA*.

Question 2.2: Does your proposed or existing information system, technology or program involve personal health information to which *PHIPA* applies? Personal health information means identifying information about an individual in oral or recorded form that:

(i) relates to his/her physical or mental health;
(ii) relates to providing health care, including identifying a provider of health care;
(iii) is a plan of service within the meaning of the Long-Term Care Act, 1994;
(iv) relates to the donation of a body part or bodily substance;
(v) relates to payments or eligibility for health care in respect of the individual;
(vi) is a health number;
(vii) identifies a substitute decision-maker of that individual; or,
(viii) is in a record where the record contains any of the above information.

Personal health information does not include a record of information about an employee or other agent of the health information custodian, unless the record is primarily related to the provision of health care to the employee or agent. *PHIPA* also does not apply to all personal health information, but only to that which is: (i) collected, used or disclosed by health information custodians; or, (ii) used or disclosed by persons who receive personal health information from health information custodians. See Appendix C for a complete definition of personal health information, as defined by *PHIPA*.

2.3 Are you a health information network provider under *PHIPA*?

The IPC recognizes that privacy impact assessments are not formally required under *PHIPA*, unless an organization is classified as a "health information network provider." A health information network provider is defined as a person (which includes organizations) "who provides services to two or more health information custodians where the services are provided primarily to health information custodians to enable the health information custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians."[9] An example of a health information network provider under *PHIPA* is the Ontario Smart Systems for Health Agency.

If you are a health information network provider, you are required, pursuant to section 6(3) of Ontario Regulation 329/04 of *PHIPA*, to "perform, and provide to each applicable health information custodian a written copy of the results of, an assessment of the services provided to the health information custodians, with respect to:

i. threats, vulnerabilities and risks to the security and integrity of the personal health information; and
ii. how the services may affect the privacy of the individuals who are the subject of the information."

You are not required to provide a copy of your PIA to the IPC. Health information network providers must also follow a number of other requirements prescribed under section 6(3) of Regulation 329/04 of *PHIPA*, including to:

- Notify every health information custodian at the first reasonable opportunity if it accessed, used, disclosed or disposed of personal health information in an unauthorized manner;
- Provide to each health information custodian a plain language description of the services provided and safeguards that have been implemented to protect personal health information against unauthorized use or disclosure;
- Make available to the public a plain language description of the services provided and safeguards that have been implemented to protect personal health information against unauthorized use or disclosure and any directives, guidelines and policies that apply to the services provided;
- Retain and provide to the health information custodian, upon request, an electronic record of all accesses and transfers of personal health information associated with the health information custodian;
- Ensure that any third parties retained to provide or assist in providing services also comply with the necessary restrictions and conditions to allow providers to comply with its requirements; and
- Enter into a written agreement with each health information custodian describing the services provided; the administrative, technical and physical safeguards in place to protect the confidentiality and security of the personal health information; and that requires the provider to comply with *PHIPA* and its regulations.

As noted earlier, the IPC strongly recommends that health information custodians conduct a PIA on proposed or significant existing information systems, technologies or programs involving personal health information to identify and mitigate privacy risks, *even if they are not a health information network provider who is formally required to conduct a* PIA *under PHIPA*. These guidelines will assist health information custodians in this regard.

9 *Personal Health Information Protection Act, 2004*, Ontario Regulation 329/04, section 6(2)

3 QUESTIONNAIRE INSTRUCTIONS

3.1 Understanding how the questionnaire is organized

If you have determined that your organization is a health information custodian and that the proposed or existing information system, technology or program with which are you dealing involves personal health information as defined under *PHIPA* (see sections 2.1 and 2.2 above), then you are now ready to complete the PIA questionnaire.

The questions you will see in the *PIA Guidelines* ask for information in two forms. First, the health information custodian must complete checkboxes, which provide summary responses to the questions posed in the questionnaire. The categories for the checkboxes are:

- "Yes"
- "In Progress"
- "No"
- "N/A" ("Not Applicable" or "Not Available").

Second, "note fields" or free text fields provide for elaboration of responses to the checkboxes as the health information custodian feels is appropriate. In addition, the questionnaire has a column to provide for cross-references to separate enclosures on specific responses, which the health information custodian may wish to include as supporting information. Examples of separate enclosures may include written materials about the information system, technology or program, such as the business case, project charter, technical specifications, excerpts from system manuals and interviews with relevant personnel, including vendors where appropriate. This type of information should be cited in the "Enclosure Reference" column. The health information custodian may use the note fields and enclosures in combination or interchangeably. The PIA questionnaire can be completed in paper or electronic format (see Appendix A – PIA Questionnaire Template for blank template of the PIA Questionnaire).

3.2 "Note fields" versus "enclosure references"

Whether you choose to provide your answers to the questions in the note fields or in separate enclosures is unimportant. What is important, however, is to do more than simply check off a "Yes," "No," "In Progress" or "N/A" in the questionnaire's checkboxes. In other words, you should use the note fields, the separate enclosures or both, but do **NOT** simply fill in the checkboxes and fail to provide any information about why you have made certain choices for those checkboxes. One of the characteristics of a valuable PIA is that it not only clearly states how personal health information for an information system, technology or program is or will be collected, used, disclosed, retained and protected but it also clearly explains why the personal health information is or will be collected, used, disclosed, retained and protected in certain ways, and what broader organizational privacy management practices are in place to support those choices. In most cases, only supplementary information provided in the note fields and/or in separate reference enclosures will fulfil the latter requirement.

3.3 Organizational privacy management versus project privacy management

The questionnaire is broken into two parts: Part A, Organizational Privacy Management, and Part B, Project Privacy Management. Part A relates to the health information custodian's information practices as a whole, while Part B relates specifically to the privacy practices of the proposed or existing information system, technology or program for which the PIA is being completed. Once a health information custodian has completed the entire questionnaire once for any information system, technology or project, Part A will likely only need to be revised for continued accuracy during the completion of each subsequent PIA, not completed anew.

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
	Questionnaire "part" and question number.	Check the box in this column if your response is "Yes" and then explain your answer in the notes field or indicate where additional information can be found in a separate enclosure in the "Enclosure Reference" field.	Check the box in this column if you are in the process of determining the response. Be sure to provide elaboration of any responses in this column.		Check the box in this column if your response is "No" and then explain your answer in the notes field or with a separate enclosure.	
A1	Does your organization have a written privacy policy or statement of information practices?					

Note:

As mentioned above, it is important that you elaborate upon your response, wherever possible. The notes field is the location where you will provide a more detailed explanation of your response. If you are using the electronic version of the PIA questionnaire, simply select notes field and insert the text. This field will expand to hold unlimited explanatory text. If you are completing a paper version, you will likely need to append your response to the questionnaire.

Check the box in this column if the question is not applicable to your organization or the information system, technology or program in question, or if the requested information is not available. Be sure to provide elaboration on any question when the N/A box is selected.

Indicate the number or specific reference to a separate enclosure or part of a separate enclosure related to your response in this field. Each separate enclosure should be referenced at least once in the questionnaire. Be as specific as possible with the reference (for example, indicate page number(s) where applicable). Typically, enclosed documents should include your organization's description of information practices or privacy policy (or policies), written public statement, any relevant project materials, such as project charters and data flow diagrams, and relevant excerpts from your organization's Information Management or Information Technology (IM/IT) strategic plan.

4 PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE – ANNOTATED[10]

In addition to the responses you will provide to the questions in the PIA questionnaire below, your PIA should include the following information:

- The name of the information system, technology or program for which the PIA is being prepared;
- The date the author of the PIA completes the questionnaire;[11]
- The name of the health information custodian with responsibility or control of the information system, technology or program; and
- The contact information for the author of the PIA, including his or her name, title, mailing address, telephone and fax numbers and e-mail address. This information is especially important to include in the PIA if it will be reviewed by external stakeholders, such as other health information custodians, patients/clients or other community representatives. The contact person should be capable of responding to detailed questions concerning the PIA or identifying persons who can.

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
	Remember to identify the relevant section or page(s) of your enclosure package in the "Enclosed Reference" column whenever you provide an enclosure. You may want to number the pages of your enclosure sequentially from beginning to end, for ease of reference. This is especially important if external stakeholders will be reviewing your PIA, since these individuals are less likely to be familiar with the details of the proposed information system, technology or program.					
	Part A: Organizational Privacy Management **The questions in this section relate to privacy management throughout your organization. They are not limited to the information system, technology or program. Specific questions related to the information system, technology or program appear in Section B.**					
A1	**Is there an organizational strategic plan or business plan that addresses privacy protection?**					

[10] A blank template of the PIA questionnaire can be found in Appendix A.

[11] It is the Commissioner's view that a PIA is rarely ever finished. It is a dynamic document that should be updated regularly as changes are contemplated for the information system, technology or program.

#	Question	Yes	In Progress	No	N/A	Enclosed Reference

Note: Often health information custodians address privacy considerations in their information management/information technology plans. Some health information custodians may also have departmental business or strategic plans; if such plans address privacy issues, they may also be enclosed. (E.g. a business plan for a new health information system, a new clinical department, a new fundraising initiative or a new research program may include information that addresses privacy protection).

A2 Does your organization have a written privacy policy or statement of information practices?

Note: Question A1 refers to organizational plans that include privacy measures; this question refers to a policy or mission statement that is specifically related to the information handling practices and protection of privacy at your organization. Such documents are often referred to as privacy or information practices policies or charters and are required under section 10 of *PHIPA*. Documents that are responsive to this question will normally apply to the entire organization, not to a specific business area or project.

A3 Have privacy policies or procedures been developed for various aspects of the organization's operations?

Note: This question relates to privacy-related policies or procedures applying to specific aspects of the organization's operations. Such policies or procedures, if they exist, are typically separate from organization-wide privacy policies or charters, which are dealt with in question A2. Privacy policies or procedures applying to specific aspects of the organization's operations may form part of the broader policies or procedures dealt with in question A2. If so, please indicate in "encl. ref." field where in the enclosure this information may be found.

A4 Do the privacy policies or procedures that you identified in response to questions A2 and A3 ensure the following:

- Personal health information is collected in accordance with *PHIPA* and other applicable legislation;
- Individual consent is obtained in accordance with section 18 of *PHIPA* where consent is required;

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
	• A written public statement about the organization's information practices, who to contact with privacy questions or complaints, and how to obtain access or request correction of a record of personal health information, is readily available to individuals as outlined in section 16 of *PHIPA;* • Individuals are entitled to request access to and correction of their own personal health information as provided for under sections 52-55 of *PHIPA*, subject to certain exceptions; • There is a record retention schedule for records of personal health information that outlines the minimum and maximum lengths of time personal health information may be retained as well as procedures outlining the manner by which personal health information will be securely destroyed.					

Note: This question relates to several key aspects of the contents of various policies or procedures that may have been identified in questions A2 and A3. The individual points in this question are key elements of *PHIPA* and are generally accepted fair information practices.

A5	Are administrative, technical and physical safeguards in place at the organization to protect personal health information against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal pursuant to section 12 of *PHIPA*?					

Note: This question relates to whether or not your organization has in place administrative, technical and physical safeguards, which are critical to minimizing privacy risks and protecting the confidentiality and integrity of personal health information. If your organization has developed an information security plan or policy, you should enclose a copy of the plan in your PIA in response to this question.

***If your organization adheres to a generally accepted industry or government standard for information security, such as ISO 17799, you should identify that standard in your elaboration for this question and indicate whether your organization has been certified.*

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
	Privacy Structure and Organization					
A6	Is there an appointed privacy contact person in the organization?					

Note: If no person has been assigned overall responsibility for privacy issues in the organization, check "No." However, note that section 15 of *PHIPA* requires health information custodians to have a privacy contact person. If your organization has identified a privacy contact person, you should specify in the notes field which position has been designated as the person with overall responsibility for privacy issues (e.g. Chief Privacy Officer, Chief Information Officer, etc.).

A7	Does a reporting process exist to ensure that the organization's management is informed of any privacy compliance issues?					

Note: If a policy or procedure exists to report privacy compliance issues, you should enclose a copy of this policy or procedure in your PIA. If not, your PIA should describe how, when and at what level management would be informed of any alleged or actual failures to comply with *PHIPA*, other applicable legislation or policies in regard to privacy protection.

A8	Are senior executives actively involved in the development, implementation and/or promotion of your organization's privacy program?					

Note: If senior executives are involved in your organization's privacy program, you should describe the nature of their involvement. If your organization has a privacy contact person, you should also describe the nature of his or her reporting relationship and position within the organization, including how closely he or she works with your organization's senior executives.

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
A9	Are employees or agents with access to personal health information in your organization provided with training related to privacy protection?					

Note: This question relates mainly to general training within the organization, such as new employee orientations and general *PHIPA* training, but also includes such safeguards as requiring employees or agents to sign confidentiality agreements as a condition of employment. If your organization does not have any form of privacy training in place, select "no." However, note that one of the responsibilities of your organization's privacy contact person (see question A6) is to ensure agents are appropriately informed of their duties under *PHIPA*. Your PIA should identify any privacy-related training that your organization's employees or agents undergo. Specific training information related to the information system, technology or program should be provided in response to question B15. The information you provide on privacy training should note the length and frequency of training, which categories of employees or agents receive training, and how the organization documents the fact that an employee or agent has received privacy training.

A10	Have policies and procedures been developed concerning the management of privacy breaches, including the notification of individuals when the confidentiality of their personal health information has been breached?					

Note: This question relates to the process following the determination that an inappropriate use or disclosure of personal health information has occurred. Such policies will typically outline the reporting and accountability structure for a breach as well as notifying individuals whose personal health information was the subject of the breach. Section 12(2) of *PHIPA* requires that health information custodians notify individuals at the first reasonable opportunity if their personal health information is stolen, lost, or accessed by unauthorized persons.

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
	Part B: Project Privacy Management **The questions in this section relate to the information system, technology or program.**					
B1	Has a summary of the proposed or existing information system, technology or program been prepared, including a description of the requirements for the system, technology or program and a description of how the information system, technology or program will or does meet those needs?					

Note: This is an important enclosure because it provides the basic rationale for the proposed or existing information system, technology or program. This information would typically be included in the proposed or existing information system, technology or program's project charter, project plan, needs assessment or other material explaining why the information system, technology or program has been or will be implemented.

B2	Has a listing of all personal health information or data elements that will be or are collected, used or disclosed in the proposed or existing information system, technology or program been prepared?					

Note: This enclosure is important because it illustrates the scope and nature of personal health information involved in the proposed or existing information system, technology or program.

B3	Have diagrams been prepared depicting the flow of personal health information in the proposed or existing information system, technology or program?					

Note: There are many ways to prepare data flow diagrams, and your choice will depend in part on the nature of the information system, technology or program. The data flow diagram should illustrate how personal health information is collected, how it circulates within, and how it is disseminated beyond the proposed or existing information system, technology or program.

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
B4	Have documents been prepared showing which persons, positions, or employee categories will have access to which elements or records of personal health information?					

Note: This enclosure is important to illustrate the application of the "need-to-know" principle in *PHIPA* and to complement the data flow diagram requested in question B3. In some cases, it may be possible to incorporate this information into the information flow diagram for question B3; if you have done so, you should note that fact in your response to this question as well as question B3.

B5	Does consent from the individual or an authorized substitute decision-maker provide the primary basis for the collection, use and disclosure of personal health information for the proposed or existing information system, technology or program?					

Note: Under *PHIPA*, there are several collections, uses and disclosures of personal health information that do not require an individual's consent (see sections 36 through 50 of *PHIPA*). If individual consent does **not** form the basis for the collection, use and disclosure of personal health information, your PIA should identify the alternative authority that applies.

B6	Have you documented the purposes for which personal health information will be or is collected, used or disclosed in the information system, technology or program?					

Note: Your PIA should include any documentation which clearly sets out the purposes for which personal health information will be collected, used or disclosed. If this information has been provided in response to other questions, you may cross-reference as necessary in your PIA. This question also relates to question B5 as, in the event consent provides the basis for the collection, use or disclosure of personal health information, section 18(1)(b) of *PHIPA* requires that the consent be knowledgeable; one of the elements of a knowledgeable consent outlined in section 18(5) of *PHIPA* is that it must be reasonable in the circumstances to believe that the individual **knows the purposes** for which his or her personal health information is being collected, used or disclosed, as the case may be.

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
B7	Is personal health information collected, used, disclosed or retained exclusively for the identified purposes and for purposes that an individual would reasonably consider consistent with those purposes?					

Note: If you checked "Yes," this question will probably require little elaboration. If you checked "In Progress" or "No," you should elaborate and identify in your PIA any measures you will take to ensure that the collection, use or disclosure of personal health information is consistent with identified purposes. Note that section 10(2) of *PHIPA* requires health information custodians to comply with their information practices.

B8	Will personal health information in the proposed or existing information system, technology or program be linked or cross-referenced to other information in other information systems, technologies or programs?					

Note: If you checked "Yes" in response to this question, you should indicate how this link or cross-reference will be accomplished, who has custodianship of the information system, technology or program for which you are undertaking this PIA and an explanation of why the link or cross-reference is required, as well as the effect if such linkage or cross-reference was not possible. For the purpose of this questionnaire, "link" means to create a new combined record from two or more separate records of personal health information through the use of an identifier, and "cross-reference" means to identify a record of personal health information by using an identifier from another record of personal health information, but without creating a new record.

B9	Will personal health information collected or used in the information system, technology or program be disclosed to any persons who are not employees or agents of the responsible organization?					

Note: A "No" response to this question identifies an information system, technology or program for which personal health information is limited to the internal purposes of a single health information custodian. Such systems, technologies or programs may be contrasted with those in which personal health information serves the purposes of more than one health information custodian or, while serving one health information custodian, is disseminated beyond that health information custodian. Note also that a provider of the information system, technology or program may be a "**health information network provider**" (see section 2.3), if the information system, technology or program is provided to two or more health information custodians where the service is provided primarily to custodians in order to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the provider is an agent of any of the custodians.

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
B10	Have you made arrangements to provide full disclosure of all purposes for which the information system, technology or program will collect personal health information?					

Note: Disclosure of the purposes to which personal health information is to be put is an important privacy protection measure, especially when consent is being sought, and is a requirement of *PHIPA*. Your elaboration should identify the measures that will be taken to ensure that this information is communicated appropriately to the individuals affected by the information system, technology or program (e.g. patients or clients). Under *PHIPA*, the requirement for a consent to be knowledgeable (discussed in question B6 above) may be satisfied in part through posting or making available a notice of purposes for which personal health information will be collected, used or disclosed, as described in section 18(6) of *PHIPA*.

B11	Have communications products and/or a communications plan been developed to fully explain the information system, technology or program to individuals and how their personal health information will be protected?					

Note: Providing information to individuals whose personal health information will be collected, used or disclosed by the information system, technology or program about the technical, administrative and physical safeguards to protect their privacy and to maintain the confidentiality of their personal health information, will engender confidence in the information system, technology or program.

B12	Does the proposed or existing information system, technology or program involve the collection, use or disclosure of any personal health information beyond Ontario's borders?					

Note: The trans-border movement of personal health information raises a number of special privacy issues, among them the application of the *Personal Health Information Protection Act, 2004* and the federal *Personal Information Protection and Electronic Documents Act*, the adequacy of contractual provisions to protect privacy and the equivalence of privacy legislation in other jurisdictions. If the information system, technology or program involves the international transfer of personal health information, these issues may be further complicated. Your PIA should provide full details of any plans to transfer personal health information between Ontario and any other jurisdiction. See also Appendix D – Organization for Economic Co-operation and Development – Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
B13	Has an assessment been completed to identify potential risks to the privacy of individuals whose personal health information is collected, used, retained or disclosed by the proposed or existing information system, technology or program?					

Note: A critical part of a PIA is a review of the possible impact that the proposed or existing information system, technology or program may have on the privacy of individuals whose personal health information may be collected, used, retained or disclosed. This is an opportunity to consider what the overall privacy impact of the system, technology or program may be. In part, this involves identifying, from the perspective of the individuals whose personal health information is involved, how the existing or proposed system, technology or program may affect their privacy interests.

B14	If potential risks to privacy have been identified, have means to avert or mitigate those risks been incorporated into the design and/or implementation of the proposed or existing information system, technology or program?					

Note: If potential privacy risks have been identified in response to question B12 or other questions, specific measures will usually need to be taken to avert or mitigate these risks. These may include the use of privacy enhancing technologies, revising consent forms, making notices about the information system, technology or program clearer and more readily available to individuals, or implementing specific privacy training on the proposed or existing information system, technology or program. Your PIA should outline the nature of these measures in response to this question. If they have already been described in response to other questions, you may cross-reference those questions or the enclosures provided in response to those questions. Your response to this question should address any issues identified in question B12. If no response has been taken to mitigate the risks identified, you should provide a rationale for your decision in the notes field for this question.

B15	Has an assessment been completed to identify whether other health information custodians have implemented the same or a similar information system, technology or program, the risks to privacy experienced by other health information custodians and the means implemented by these other health information custodians to avert or mitigate these risks?					

#	Question	Yes	In Progress	No	N/A	Enclosed Reference

Note: Reviewing the experiences of other health information custodians who have implemented the same or similar information system, technology or program will assist in identifying the key privacy concerns and risks and how the other health information custodians have resolved a specific privacy challenge.

B16 Have key stakeholders been provided with an opportunity to comment on the sufficiency of privacy protections and their implications on the proposed or existing information system, technology or program?

Note: When a proposed or existing information system, technology or program involves large volumes of personal health information, or when that information is particularly sensitive, it is worthwhile to consult those who have privacy interests in the project. If this has been done, your PIA should provide a description of the results of such consultations.

B17 Will users be trained in the requirements for protecting personal health information and will they be made aware of the relevant notification procedures if personal health information is stolen, lost or accessed by unauthorized persons?

Note: Your PIA should describe your plans for training related to the privacy and security measures and policies your organization plans to implement for the proposed or existing information system, technology or program. Ensuring your agents are made aware of their data protection obligations will help ensure that the operations of the proposed or existing information system, technology or program comply with *PHIPA*, including section 17(3), which requires agents of a health information custodian to notify the health information custodian at the first opportunity if personal health information handled by the agent on behalf of the health information custodian is stolen, lost or accessed by unauthorized persons. Note that this question deals with specific training for the proposed or existing system, technology or program – more general privacy training programs should be described in response to question A9.

B18 Have security policies and procedures to protect personal health information against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal been documented?

#	Question	Yes	In Progress	No	N/A	Enclosed Reference

Note: Your PIA should include copies of security policies and procedures related to the management of personal health information in conjunction with the proposed or existing information system, technology or program. To the extent that you are relying on organization-wide security policies and procedures, your PIA should note this and make reference to any relevant enclosures provided in response to question A5.

B19 Have privacy policies or procedures been developed for various aspects of the operations for the proposed or existing information system, technology or program?

Note: This question relates to privacy-related policies or procedures applying to specific aspects of the operations for the proposed or existing information system, technology or program – see question B18 for more information. Your response to this question and to question B17 may overlap with your response to questions A3 and A4; if so, you should cross-reference as necessary in your PIA.

B20 Do the privacy policies or procedures that you identified in question B16 ensure the following (if so, please enclose):

- Personal health information in the proposed or existing information system, technology or program is collected in accordance with *PHIPA* and other applicable legislation;
- Individual consent is obtained in accordance with section 18 of *PHIPA* for the proposed or existing information system, technology or program where consent is required;
- A written public statement about the purposes for which the proposed or existing information system, technology or program collects, uses or discloses personal health information is readily available to individuals as outlined in section 16 of *PHIPA;*
- Individuals are entitled to request access to and correction of their own personal health information in the proposed or existing information system, technology or program, as provided for under sections 52-55 of *PHIPA*, subject to certain exceptions.

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
	• There is a record retention schedule for records of personal health information that outlines the minimum and maximum lengths of time personal health information may be retained in the proposed or existing information system, technol ogy or program, as well as procedures outlining the manner by which personal health information in the proposed or existing information system, technology or program may be securely destroyed.					

Note: This question relates to several key aspects of the contents of various policies or procedures relating to the proposed or existing information system, technology or program that may have been identified in question B17. The individual points in this question are key elements of *PHIPA* and are generally accepted fair information practices.

B21 Does the proposed or existing information system, technology or program provide functionality for the logging of the insertion, access, modification or disclosure of personal health information as well as an interface to audit those logs for unauthorized activities?

Note: This question relates to the technical capability to monitor unauthorized use of the proposed or existing information system, technology or program. Logging and auditing user activities is required to protect against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal. If your answer to this question is "yes," you should provide a general description of this functionality as well as a description of your auditing procedures. If your answer is "no" to this question, you should provide an explanation as to why the proposed or existing information system, technology or program does not include such features and what alternative means you will or have already put in place to safeguard against the unauthorized insertion, access, modification or disclosure of personal health information.

B22 Have policies and procedures been developed for the enforcement of privacy rules relating to the proposed or existing information system, technology or program, including fulfilment of the commitments made in the PIA?

Note: A number of commitments regarding the proposed or existing information system, technology or program will have been made in responses to this questionnaire. Statements of policy and procedure will have been provided. Security measures will have been described. Other measures to protect privacy will also have been identified. This question seeks information concerning how the organization will demonstrate its compliance with (a) the requirements in *PHIPA* and other legislative obligations, and (b) its own commitments. Your PIA should elaborate as necessary to describe how audit, compliance and enforcement will be achieved.

Appendix A – PIA Questionnaire Template

Name of the information system, technology or program for which the PIA is being prepared:

Date:

Name of the health information custodian
with responsibility or control of the information system, technology or program:

Author's name:

Author's title:

Author's mailing address:

Author's telephone number:

Author's fax number:

Author's e-mail address:

#	Question	Yes	In Progress	No	N/A	Enclosed Reference

Remember to identify the relevant section or page(s) of your enclosure package in the "Enclosed Reference" column whenever you provide an enclosure. You may want to number the pages of your enclosure sequentially from beginning to end, for ease of reference. This is especially important if external stakeholders will be reviewing your PIA, since these individuals are less likely to be familiar with the details of the information system, technology or program.

Part A: Organizational Privacy Management

The questions in this section relate to privacy management throughout your organization. They are not limited to the information system, technology or program. Specific questions related to the information system, technology or program appear in Section B.

A1 Is there an organizational strategic plan or business plan that addresses privacy protection?

Note:

A2 Does your organization have a written privacy policy or statement of information practices?

Note:

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
A3	Have privacy policies or procedures been developed for various aspects of the organization's operations?					
	Note:					
A4	Do the privacy policies or procedures that you identified in response to questions A2 and A3 ensure the following: • Personal health information is collected in accordance with *PHIPA* and other applicable legislation; • Individual consent is obtained in accordance with sections 18 of *PHIPA* where consent is required; • A written public statement about the organization's information practices, who to contact with privacy questions or complaints, and how to obtain access or request correction of a record of personal health information is readily available to individuals, as outlined in section 16 of *PHIPA*; • Individuals are entitled to request access to and correction of their own personal health information as provided for under sections 52-55 of *PHIPA*, subject to certain exceptions; • There is a record retention schedule for records of personal health information that outlines the minimum and maximum lengths of time personal health information may be retained as well as procedures outlining the manner by which personal health information will be securely destroyed.					
	Note:					
A5	Are administrative, technical and physical safeguards in place at the organization to protect personal health information against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal pursuant to section 12 of *PHIPA*?					

#	Question	Yes	In Progress	No	N/A	Enclosed Reference

Note: "If your organization adheres to a generally accepted industry or government standard for information security, such as ISO 17799, you should identify that standard in your elaboration for this question and indicate whether your organization has been certified.

A6 Is there an appointed privacy contact person in the organization?

Note:

A7 Does a reporting process exist to ensure that the organization's management is informed of any privacy compliance issues?

Note:

A8 Are senior executives actively involved in the development, implementation and/or promotion of your organization's privacy program?

Note:

A9 Are employees or agents with access to personal health information in your organization provided training related to privacy protection?

Note:

A10 Have policies and procedures been developed concerning the management of privacy breaches, including the notification of individuals when the confidentiality of their personal health information has been breached?

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
	Note:					
	Part B: Project Privacy Management **The questions in this section relate to the information system, technology or program.**					
	Project Description					
B1	Has a summary of the proposed or existing information system, technology or program been prepared, including a description of the requirements for the system, technology or program and a description of how the information system, technology or program will or does meet those needs?					
	Note:					
B2	Has a listing of all personal health information or data elements that will be or are collected, used or disclosed in the proposed or existing information system, technology or program been prepared?					
	Note:					
B3	Have diagrams been prepared depicting the flow of personal health information in the proposed or existing information system, technology or program?					
	Note:					
B4	Have documents been prepared showing which persons, positions, or employee categories will have access to which elements or records of personal health information?					

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
	Note:					
B5	Does consent from the individual or an authorized substitute decision-maker provide the primary basis for the collection, use and disclosure of personal health information for the proposed or existing information system, technology or program?					
	Note:					
B6	Have you documented the purposes for which personal health information will be or is collected, used or disclosed in the information system, technology or program?					
	Note:					
B7	Is personal health information collected, used, disclosed or retained exclusively for the identified purposes and for purposes that an individual would reasonably consider consistent with those purposes?					
	Note:					
B8	Will personal health information in the proposed or existing information system, technology or program be linked or cross-referenced to other information in other information systems, technologies or programs?					
	Note:					

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
	Note:					
B9	Will personal health information collected or used in the information system, technology or program be disclosed to any persons who are not employees or agents of the responsible organization?					
	Note:					
B10	Have you made arrangements to provide full disclosure of all purposes for which the information system, technology or program will collect personal health information?					
	Note:					
B11	Have communications products and/or a communications plan been developed to fully explain the information system, technology or program to individuals and how their personal health information will be protected?					
	Note:					
B12	Does the proposed or existing information system, technology or program involve the collection, use or disclosure of any personal health information beyond Ontario's borders?					
	Note:					

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
B13	Has an assessment been completed to identify potential risks to the privacy of individuals whose personal health information is collected, used, retained or disclosed by the proposed or existing information system, technology or program?					
	Note:					
B14	If potential risks to privacy have been identified, have means to avert or mitigate those risks been incorporated into the design and/or implementation of the proposed or existing information system, technology or program?					
	Note:					
B15	Has an assessment been completed to identify whether other health information custodians have implemented the same or a similar information system, technology or program, the risks to privacy experienced by other health information custodians and the means implemented by these other health information custodians to avert or mitigate these risks?					
	Note:					
B16	Have key stakeholders been provided with an opportunity to comment on the sufficiency of privacy protections and their implications on the proposed or existing information system, technology or program?					
	Note:					

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
B17	Will users be trained in the requirements for protecting personal health information and will they be made aware of the relevant notification procedures if personal health information is stolen, lost or accessed by unauthorized persons?					
	Note:					
B18	Have security policies and procedures to protect personal health information against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal been documented?					
	Note:					
B19	Have privacy policies or procedures been developed for various aspects of the operations for the proposed or existing information system, technology or program?					
	Note:					
B20	Do the privacy policies or procedures that you identified in question B16 ensure the following (if so, please enclose): • Personal health information in the proposed or existing information system, technology or program is collected in accordance with *PHIPA* and other applicable legislation;					

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
	• Individual consent is obtained in accordance with section 18 of *PHIPA* for the proposed or existing information system, technology or program where consent is required;					
	• A written public statement about the purposes for which the proposed or existing information system, technology or program collects, uses or discloses personal health information is readily available to individuals as outlined in section 16 of *PHIPA;*					
	• Individuals are entitled to request access to and correction of their own personal health information in the proposed or existing information system, technology or program as provided for under sections 52-55 of *PHIPA*, subject to certain exceptions;					
	• There is a record retention schedule for records of personal health information that outlines the minimum and maximum lengths of time personal health information may be retained in the proposed or existing information system, technology or program, as well as procedures outlining the manner by which personal health information in the proposed or existing information system, technology or program may be securely destroyed.					
	Note:					
B21	Does the proposed or existing information system, technology or program provide functionality for the logging of the insertion, access, modification or disclosure of personal health information as well as an interface to audit those logs for unauthorized activities?					
	Note:					

#	Question	Yes	In Progress	No	N/A	Enclosed Reference
B22	Have policies and procedures been developed for the enforcement of privacy rules relating to the proposed or existing information system, technology or program, including fulfilment of the commitments made in the PIA?					

Note:

Appendix B – Sample Methodologies for Conducting a PIA

Canada

- Information and Privacy Commissioner/Ontario, *Privacy Diagnostic Tool*; *http://www.ipc.on.ca/userfiles/page_attachments/pdt.pdf*
- Ontario, Management Board Secretariat, *Privacy Impact Assessment Guidelines* (June, 2001); *http://www.gov.on.ca/MBS/english/fip/pia/*
- Ontario Management Board Secretariat, *Model Cross-Jurisdictional Privacy Impact Assessment Guide* (Draft, October, 1999); *http://www.gov.on.ca/MBS/english/fip/pub/fed_pia.html*
- Treasury Board of Canada Secretariat, *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks* (August, 2002); *http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1_e.asp*
- Office of the Information and Privacy Commissioner of Alberta, *Privacy Impact Assessment: Full Questionnaire*; *http://www.oipc.ab.ca/ims/client/upload/piaform-full.pdf*
- Alberta Medical Association, *Guide to Privacy Impact Assessments for Physicians Offices* (February, 2002); *http://www.albertadoctors.org/advocacy/healthinfo/privacy_impact_statements.htm*

International

- Privacy Commissioner/New Zealand, *Privacy Impact Assessment Handbook* (March, 2002, Auckland, 40 pp.); *www.privacy.org.nz/comply/pia.html*
- U.S. Department of Interior, *Privacy Impact Assessment and Guide* (September, 2002); *http://www.doi.gov/ocio/cp/Privacy%20Impact%20Assessment_9.16.02.pdf*
- U.S. Internal Revenue Service. *Model Information Technology Privacy Impact Assessment* (February, 2000); *http://www.cio.gov/documents/pia_for_it_irs_model.pdf*
- U.S. Department of Justice, Office of Justice Programs, *Privacy Impact Assessment for Justice Information Systems* (February, 2001); *http://it.ojp.gov/initiatives/files/Privacy3.pdf*

Appendix C – Definition of "Personal Health Information" under *PHIPA*

Section 4 of the *Personal Health Information Protection Act, 2004* defines personal health information to mean:

Personal health information means "identifying information" about an individual in oral or recorded form, if the information:

(a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family;

(b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual;

(c) is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual;

(d) relates to payments or eligibility for health care in respect of the individual;

(e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance;

(f) is the individual's health number; or

(g) identifies an individual's substitute decision-maker.

"Identifying information" means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

Personal health information does not include identifying information contained in a record that is in the custody or under the control of a health information custodian if,

(a) the identifying information contained in the record relates primarily to one or more employees or other agents of the custodian; and

(b) the record is maintained primarily for a purpose other than the provision of health care or assistance in providing health care to the employees or other agents.

For example, a doctor's note to support an absence from work in the personnel file of a secretary employed by a health information custodian is not considered personal health information.

Appendix D – Organization for Economic Co-operation and Development – Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

For more information, see the OECD web site at *www.oecd.om.*

Preface

The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills) to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data.

On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

For this reason, OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it.

The Guidelines, in the form of a Recommendation by the Council of the OECD, were developed by a group of government experts under the chairmanship of The Hon. Mr. Justice M.D. Kirby, Chairman of the Australian Law Reform Commission. The Recommendation was adopted and became applicable on 23rd September, 1980.

The Guidelines are accompanied by an Explanatory Memorandum intended to provide information on the discussion and reasoning underlining their formulation.

Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

September 23, 1980

The Council,

Having regard to articles 1(c), 3(a) and 5(b) of the Convention on the Organization for Economic Co-operation and Development of 14th December, 1960;

Recognizing:

that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

that transborder flows of personal data contribute to economic and social development;

that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

Recommends:

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;

2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;

3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;

4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

Annex to the Recommendation of the Council of September 23, 1980

PART ONE: GENERAL

Definitions

1. For the purposes of these Guidelines:

   a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;

   b) "personal data" means any information relating to an identified or identifiable individual (data subject);

   c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

   a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

   b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

   c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

   a) as few as possible; and
   b) made known to the public.

5. In the particular case of Federal countries, the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

Part Two: Basic Principles of National Application

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

    a) with the consent of the data subject; or
    b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him
- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Part Three: Basic Principles of International Application: Free Flow and Legitimate Restrictions

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

Part Four: National Implementation

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:
    a) adopt appropriate domestic legislation;
    b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
    c) provide for reasonable means for individuals to exercise their rights;
    d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
    e) ensure that there is no unfair discrimination against data subjects.

Part Five: International Co-operation

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:
    - information exchange related to these Guidelines; and
    - mutual assistance in the procedural and investigative matters involved.

Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

Notes

Notes

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto (Ontario) M4W 1A8
Telephone : 416 326-3333 *or* 1 800 387-0073
Fax : 416 325-9195
TTY : 416 325-7539
Web site : www.ipc.on.ca
Email : info@ipc.on.ca